PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-110491
(43)Date of publication of application : 23.04.1990

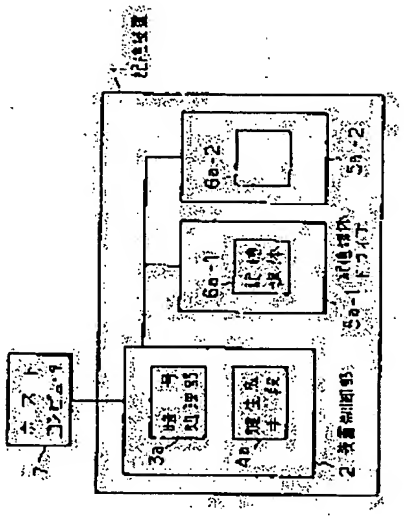
(51)Int.Cl. G09C 1/10
G06F 12/14

(21)Application number : 63-264940
(22)Date of filing : 19.10.1988

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MIYAGUCHI SHOJI
IWATA MASAHIKO

(54) STORAGE DEVICE

(57)Abstract:
PURPOSE: To use different keys to each storing medium FDi and to improve the security of a storage device by storing identifying names on a recording medium and deciding the keys by using secret parameters.
CONSTITUTION: This storage device 1 is constituted of recording medium drives 51-1 and 5a-2 and a device controlling section 2. Plural recording media 6a-1 and 6a-2 are represented as FDi (i=1, 2,...) which respectively have and store identifying names IDi and protective codes Gi. Then keys Ki used for ciphering and deciphering data stored on the recording media 6a-1 and 6a-2 are fixed as Ki=F(SGi, IDi). The S.Gi is SGi=fx&Agr; (S,Gi), the F, fx, and S of which respectively represent the key preparing algorithm held by the storage device, internal function of the F, and secret parameter of the F. Therefore, individual keys can be used for the storing media 6a-1 and 6a-2 without using any key management file and the storing content of the storage device can be ciphered and deciphered.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−110491

⑤Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)4月23日
G 09 C 1/10		7368−5B	
G 06 F 12/14	320 B	7737−5B	

審査請求　未請求　請求項の数 2　(全4頁)

⑤発明の名称　記憶装置

⑳特　願　昭63−264940
㉒出　願　昭63(1988)10月19日

㉗発明者　宮口　庄司　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
㉗発明者　岩田　雅彦　東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内
㉗出願人　日本電信電話株式会社　東京都千代田区内幸町1丁目1番6号
㉔代理人　弁理士　草野　卓

明　細　書

1. 発明の名称

記憶装置

2. 特許請求の範囲

(1) 記憶媒体FDiに対し読み書きを行う記憶装置において、

上記記憶媒体FDiは識別名称IDiを有し、

鍵Kiを生成する鍵生成手段と、

その鍵Kiにより上記記憶媒体FDi内のデータを暗号化および復号化する暗号処理部とを備え、

上記鍵生成手段は

$$Ki = P(S, IDi)$$

Pは鍵生成手段の機能を表すアルゴリズム、Sは Pの秘密パラメータ、により鍵Kiを決めるものであることを特徴とする記憶装置。

(2) 上記記憶媒体FDiは保護コードFCiをも有し、鍵生成手段の機能を表すアルゴリズムは$Ki=P(SCi, IDi)$、但し$SCi = f_s(S, Ci)$、f_sはPの内部関数であることを特徴とする請求項1記載の記憶装置。

3. 発明の詳細な説明

「産業上の利用分野」

この発明は、記憶媒体の内容を暗号化及び復号化する機能を有する記憶装置に関するものである。

「従来の技術」

従来における記憶媒体FDの暗号化鍵の決定方法は、次の通りである。

例1：全て同じ鍵を使う。この方法は鍵が一旦他人に知られると全ての記憶媒体FDの内容を復号化されてしまうという欠点がある。

例2：各FD毎に異なる個別鍵を使う。個別鍵は、鍵管理簿を作って管理する。

この方法では、記憶装置は記憶媒体FDの個数だけ鍵を保有する必要があるため、記憶媒体FD数の増加と共に鍵の管理コストが大きくなる欠点がある。

この発明の目的は、鍵管理簿を使わずに各記憶媒体FD毎に異なる個別鍵を使用し、記憶媒体FDの内容を暗号化及び復号化する機能を有する記憶装置を提供することにある。

「課題を解決するための手段」

記憶装置は、記憶媒体ドライブFDDと装置制御部とから成る。情報を記憶する記憶媒体FDは、記憶媒体ドライブFDDに着脱可能または固定である。複数の記憶媒体FDをFDi、i=1,2,…、で表す。

各FDiは、その識別名称IDiと保護コードGiを持ち、IDiとGiをその内部に記憶する。IDiとGiは、暗号化と復号化の対象としない。

記憶媒体FDに記憶するデータ(IDiとGiを除く)を暗号化及び復号化する鍵Kiは、次の様に定める。

Ki=F(SGi,IDi)

但し、SGi=f_x(S,Gi)

ここで、Fは記憶装置が有する鍵生成アルゴリズム、f_xはFの内部関数、SはFの秘密パラメータである。SはFDi側に秘密とする。

(他の鍵決定方法)

上記の鍵決定方法で、保護コードGiを使わない鍵決定方法である。即ち、鍵は以下により決める。

Ki=F(S,IDi)

(アルゴリズムP(S,x_i)の作り方)

第一の方法は、暗号化アルゴリズムEを用いてアルゴリズムPを作る方法である。Pは、次のように定める。

P(S,x_i)=E(S,x_i)

即ち、アルゴリズムPの秘密のパラメータSを鍵として、識別名称IDiを平文データと見なして暗号化する。ここでE(K,P)は鍵をKとしてPを平文データとして暗号化した暗号文を表す。識別名称IDiが長い場合は、識別名称IDiをNビットずつn個のデータに分けてCBCモードで暗号化し、最後に得られる暗号文ブロックCnを、P(S,x_i)の出力とする(CBCモードは国際規格ISO8372により定義される)。

第二の方法は、ハッシュ関数を用いてアルゴリズムを作る方法である。ここでハッシュ関数は以下に述べるものである。

Hu=f(Hu,Hu-1)、u=1,2,…,n

Hu:データブロック、Ho=初期値(零など)

ここで、HuやHuは、Nビットの長さがある。fは、HuとHu-1を入力変数とし、Nビット長データを出力する形式の関数である。上述した識別名称IDiをNビットずつn個のデータに分け、左から順にXi1,Xi2 …,Xinとおき、Hu=Xiu,Ho=Sとして、ハッシュ関数により順次計算し、最後に得られるHnを、アルゴリズムP(S,Xi)の出力とする。

Fの内部関数f_xは、例えばf_x(S,Gi)=S⊕Gi,或は、f_x(S,Gi)=(S‖Gi)⊕q(⊕はビット対応の排他的論理和,‖はデータの連結、qは秘密の定数)として決めるが、内部関数f_xはSとGiの関数であれば適当に決めて良い。

「実施例1」

第1図により説明する。記憶装置1は装置制御部2、記憶媒体ドライブ5a-1、5a-2から成る。装置制御部2は、内部にS保持手段、物理保護手段、鍵生成手段4a、暗号処理部3aを有する。記憶媒体ドライブ5a-j(j=1,2)には、記憶媒体6a-i(i=1,2)が着脱可能または固定である(第1図は記憶媒体を記憶媒体ドライブに装着した図である)。ホストコンピュータ7は、記憶装置1とデータの授受を行う。

S保持手段は、例えばバッテリバックアップによりパラメータSを常時メモリに記憶しておく。物理保護手段は、例えば物理鍵を付加することによりパラメータSの投入を制限し、またSを外部に読み出せない性質を持たせる。鍵生成手段4aは、パラメータSをS保持手段から入力し、識別名称IDiと保護コードGiを記憶媒体FDiから入力し、鍵Kiを生成し、この結果を暗号処理部3aに伝える。暗号処理部3aは、鍵生成手段4aから鍵Kiを受け取り、対象とするデータを暗号化または復号化する。

この記憶装置を動作させるためには、まず、準備として物理鍵を所有するシステム管理者がS保持手段に秘密パラメータSを入力しておく。次に、暗号化及び復号化により以下の手順に従う。

(暗号化の場合)

ホストコンピュータ7からのデータを記憶すべき記憶媒体FDi、6a-iを記憶媒体ドライブ5a-jに装着する(FDiが記憶媒体ドライブに固定されている場合は除く)。装置制御部2は記憶媒体FDi、

6a-iの中の識別名称IDiと保護コードGiを読み取り、鍵生成手段4a内の鍵生成アルゴリズムFとS保持手段内に保持しているパラメータSを用い、

Ki＝F(SGi，IDi)

但し、SGi＝fx(S，Gi)

により鍵Kiを次め、得られたKiを用いてホストコンピュータ7からのデータMを暗号処理部3aにより、

C＝E(Ki，M)

と暗号化して記憶媒体FDi、6a-iに記憶する。ここで、E(k，m)は、暗号処理部3aが有する暗号化アルゴリズムであり、kは暗号化の鍵、mは平文データとする。

(復号化の場合)

記憶媒体FDi、6a-i内のデータを復号化して読み出す場合、まず、記憶媒体FDi、6a-iを記憶媒体ドライブ5a-jに装着する(FDiが記憶媒体ドライブに固定されている場合は除く)。装置制御部2は、記憶媒体FDi、6a-iの中の識別名称IDiと保護コードGiを読み取り、鍵生成手段4a内の鍵生成アルゴリズムFとS保持手段内に保持しているパラメータSを用い、

Ki＝F(SGi，IDi)

但し、SGi＝fx(S，Gi)

により鍵Kiを次め、得られたKiをもちいて記憶媒体FDi、6a-i内のデータCを暗号処理部3aにより、

M＝E⁻¹(Ki，C)

と復号化してホストコンピュータ7へ転送する。ここでE⁻¹(k，c)は、暗号処理手段3aが有する復号化アルゴリズムであり、kは復号化の鍵、cは暗号文データとする。

「実施例2」

実施例1において保護コードGiを使わない方法である。即ち、

Ki＝F(S，IDi)

により鍵Kiを生成する。他は実施例1と同様である。

「実施例3」

第2図により説明する。パソコン8はパソコン主部9、記憶媒体ドライブ5b-1、5b-2から成る。パソコン主部9は内部にS保持手段、鍵生成手段4b、暗号処理部3bを有する。記憶媒体ドライブ5b-j(j＝1,2)には、記憶媒体6b-i(i＝1,2)が着脱可能または固定である(第2図は記憶媒体を記憶媒体ドライブに装着した図である)。

S保持手段は、パラメータSをメモリに記憶しておく。鍵生成手段4bは、パラメータSをS保持手段から入力し、識別名称IDiと保護コードGiを記憶媒体FDi、6b-iから入力し、鍵Kiを生成し、この結果を暗号処理部3bに伝える。暗号処理部3bは、鍵生成手段4bから鍵Kiを受け取り、対象とするデータを暗号化または復号化する。

この記憶装置を動作させるためには、まず、利用者が、各利用者ごとに秘密のパラメータSを入力し、これをS保持手段に保持する。次に、暗号化及び復号化により以下の手順に従う。

(暗号化の場合)

パソコン8上のデータを記憶すべき記憶媒体FDi、6b-iを記憶媒体ドライブ5b-jに装着する(FDiが記憶媒体ドライブに固定されている場合は除く)。パソコン主部9は、記憶媒体FDi、6b-iの中の識別名称IDiと保護コードGiを読み取り、鍵生成手段4b内の鍵

生成アルゴリズムFとS保持手段内に保持しているパラメータSを用い、

Ei = F (SGi, IDi)

但し、SGi = f x (S,Gi)

により鍵Eiを決め、得られたEiを用いて記憶媒体FDi、6b-i内のデータCを暗号処理部3bにより、

M = E⁻¹(Ei, C)

と復号化してパソコン主部9へ転送する。ここで、E⁻¹(k,c) は、暗号処理手段3bが有する復号化アルゴリズムであり、Kは復号化の鍵、Cは暗号文データとする。

「発明の効果」

この発明による記憶装置は、記憶媒体FDi毎に異なる鍵Eiが使えるので、一つの鍵Eiが第3者に知られても、別の鍵EjがEiから算出できず安全性が高い。しかも、個別鍵を保持する鍵ファイルは不要で、鍵管理が簡単である。

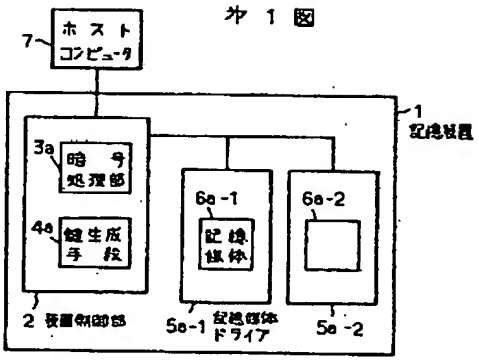
4. 図面の簡単な説明

第1図は、この発明に基づく記憶装置の第1、第2の実施例のブロック図、第2図は、この発明に基づく記憶装置の第3の実施例のブロック図である。

特許出願人　日本電信電話株式会社

代理人　卓野　卓

第1図



第2図